UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/799,860	03/12/2004	Vipul V. Prakash	CLDM-006/01US 301185-2041	1747

58249   7590   05/03/2012
COOLEY LLP
ATTN: Patent Group
Suite 1100
777 - 6th Street, NW
WASHINGTON, DC 20001

EXAMINER
SWEARINGEN, JEFFREY R

ART UNIT	PAPER NUMBER
2445	

MAIL DATE	DELIVERY MODE
05/03/2012	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

PTOL-90A (Rev. 04/07)

	Application No.	Applicant(s)
	10/799,860	PRAKASH, VIPUL V.
Office Action Summary	Examiner	Art Unit	
	Jeffrey R. Swearingen	2445	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE <u>3</u> MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.
- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
  Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1) ☒ Responsive to communication(s) filed on *25 April 2012*.

2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.

3) ☐ An election was made by the applicant in response to a restriction requirement set forth during the interview on _____; the restriction requirement and election have been incorporated into this action.

4) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

5) ☒ Claim(s) *1-9 and 12-20* is/are pending in the application.

   5a) Of the above claim(s) _____ is/are withdrawn from consideration.

6) ☒ Claim(s) *12-14* is/are allowed.

7) ☒ Claim(s) *1-9 and 15-20* is/are rejected.

8) ☐ Claim(s) _____ is/are objected to.

9) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

10) ☐ The specification is objected to by the Examiner.

11) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.

   Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

   Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

12) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

13) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

   a) ☐ All b) ☐ Some * c) ☐ None of:

   1. ☐ Certified copies of the priority documents have been received.

   2. ☐ Certified copies of the priority documents have been received in Application No. _____.

   3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

   * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08)
   Paper No(s)/Mail Date _____.

4) ☐ Interview Summary (PTO-413)
   Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Response to Arguments

1.   Applicant's arguments filed 4/25/2012 have been fully considered but they are not persuasive.

2.   Applicant argues that Mitty failed to disclose "the generation of a signature using a length of the electronic communication and the URLs extracted." Mitty [0067] states "To create the (waybill) ID, a CRC value is generated of the encrypted message M3 and a digest of the encrypted message is generated...A long version of the ID is also created (which) consists of the concatenated string of the date information, the CRC, and the digest value of the encrypted message..sender may archive the ID, the digest of the message...subject text, filenames, message length, and various information specific to the services requested."

3.   Mitty does more than archive a message length. Mitty creates a digest value (signature) of the message. The digest value includes the contents of the message, including the message length, subject text, file names, etc.

4.   Goodman disclosed extracting the URLs from electronic communications, but failed to disclose generating a signature based on the email content. However, the URL is part of the email content. Mitty generated a digest (signature) based on the entire message content, which by default included the URLs extracted by Goodman.

5.   Mitty discloses in [0032] that a "digital signature" is used to "authenticate the contents of a message and the identity of the sender...a recipient can verify that a

message has not been altered while in transit." In Mitty, a message is wrapped in a

container which also includes a digital signature – a "waybill ID".

6.　　　Applicant's main argument is that Mitty does not clearly disclose the "message

length" is used in generating the digital signature. However, in [0104] the length of the

message received at the recipient is compared with the stored "message length"

transmitted in the MIME structure which envelopes the message.

> "The logic proceeds to step 430 in which a human-readable text message and a
> computer code are generated, both corresponding to the authentication results.
> The text message and computer code are inserted, respectively, into first and
> second body parts of the M11. For example, the code and message would
> indicate that the structure having the **original message (M1)** was authenticated
> at the particular recipient 120. The computer codes may be modeled after
> S/MIME standards-related document RFC 1892. The second body part also
> includes **confirm waybill information. This information includes** the ID, the
> sequence number, the relevant e-mail addresses and certificates, service-related
> information, such as the insurance level, the filenames of any attachments, **the
> length of M1**, and time stamp information.

7.　　　Just as in [0067] where a waybill ID is created using a message length, in [0104]

the information generated at step 430 includes the original message length of M1.

8.　　　Applicant has not traversed the taking of Official Notice. Therefore the fact that

databases were stored remotely from a server is taken as Applicant Admitted Prior Art.

Allowable Subject Matter

9.　　　Claims 12-14 are allowed.

Claim Rejections - 35 USC § 103

10.　　The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all

obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set
> forth in section 102 of this title, if the differences between the subject matter sought to be patented and
> the prior art are such that the subject matter as a whole would have been obvious at the time the

invention was made to a person having ordinary skill in the art to which said subject matter pertains.
Patentability shall not be negatived by the manner in which the invention was made.

11.   Claims 1-9 are rejected under 35 U.S.C. 103(a) as being unpatentable over

Milliken et al. (US 2004/0073617) in view of Goodman et al. (US 7,711,779) in view of

Mitty et al. (US 2001/0037453)

12.   In regard to claim 1, Goodman disclosed a method comprising:

using one or more computer processors, extracting Uniform Resource Locators

from electronic communication; and (column 7, lines 56-63, identifying a spam message

based upon the presence of a URL)

analyzing the URLs extracted to determine whether the electronic communication

is of a first predetermined category, (column 7, lines 56-63)

Goodman disclosed extracting URLs from electronic communications. Goodman

disclosed determining whether a email is spam based upon the presence or absence of

a URL. Goodman failed to disclose the step of generating signatures or hash values

based upon the content of the email message.

However, Milliken disclosed generating signatures or hash values based upon

the content of the email message. Milliken, [0050], where one or more portions of a

received email are hashed to produce a hash value. Any portion of the main text, or

attachments may be hashed. The hash acts as a signature in [0052].

It would have been obvious to one of ordinary skill in the art at the time of

invention to incorporate the hashing of an email to determine whether the email

constituted spam, into the Goodman system which used the presence or absence of

URLs to determine whether an email constituted spam, in order to build a more robust spam prevention system.

Milliken failed to disclose generating a signature based upon a length of the electronic communication. Milliken did disclose hashing can be performed on "one or more header fields" of the email. [0050]. However, Mitty disclosed the generation of a "unique waybill ID" [0067] which is a CRC of the encrypted message and a digest of the encrypted message. The digest includes the "message length".

It would have been obvious to one of ordinary skill in the art at the time of invention to include a message length in the digesting/signature creation/encryption of a message in Milliken, as taught in Mitty, in order to improve the sorting techniques of Milliken in regard to building a more robust spam prevention system.

13.   In regard to claim 2, Goodman disclosed the method of claim 1, wherein extracting the URLs comprises extracting at least one of a hostname, a domain name, a subsection of a domain relative link, and an Internet Protocol (IP) address from the electronic communication. Goodman, col. 7, lines 58-63 and col. 13, lines 45-53. The elements of at least one of a hostname, a domain name, a subsection of a domain relative link, and an Internet Protocol (IP) address are inherently part of the URL as disclosed in Goodman

14.   In regard to claim 3, Milliken disclosed the method of claim 1, further comprising performing a predetermined operation on the electronic communication if the electronic communication is determined to be of the first predetermined category. [0080], rejecting message if suspicion score is high enough

15.   In regard to claim 4, Milliken disclosed the method of claim 1, wherein analyzing

the URLs comprises:

selecting one or more of the one or more signatures generated; and [0054],

storing of hash values

comparing the selected signatures against a plurality of predetermined

signatures generated from a plurality of known electronic communications of the first

predetermined category. [0082], checking hashed portions of a message with known

email lists which have been hashed

Milliken failed to teach wherein each predetermined signature of the plurality of

predetermined signatures has a signature based upon an electronic communication

length and extracted URLs. However, Goodman disclosed extracting URLs from

electronic communications. Goodman disclosed determining whether a email is spam

based upon the presence or absence of a URL. Goodman failed to disclose the step of

generating signatures or hash values based upon the content of the email message.

It would have been obvious to one of ordinary skill in the art at the time of

invention to incorporate the hashing of an email to determine whether the email

constituted spam, into the Goodman system which used the presence or absence of

URLs to determine whether an email constituted spam, in order to build a more robust

spam prevention system.

Milliken failed to disclose generating a signature based upon a length of the

electronic communication. Milliken did disclose hashing can be performed on "one or

more header fields" of the email. [0050]. However, Mitty disclosed the generation of a

"unique waybill ID" [0067] which is a CRC of the encrypted message and a digest of the encrypted message. The digest includes the "message length".

It would have been obvious to one of ordinary skill in the art at the time of invention to include a message length in the digesting/signature creation/encryption of a message in Milliken, as taught in Mitty, in order to improve the sorting techniques of Milliken in regard to building a more robust spam prevention system.

16.   In regard to claim 5, Milliken disclosed the method of claim 1, wherein generating the one or more signatures further comprises:

computing a first hash based on the length of the electronic communication; computing a second hash ...; and generating a signature by concatenating the first hash to the second hash. Milliken disclosed hashing portions of an email, [0050]. A fixed length of a hash is established in [0055]. Concatenating hashes is taught in [0086].

17.   Milliken failed to disclose an extracted URL was hashed.

18.   However, Goodman disclosed using the presence of a URL within an email to determine whether an email was spam. Goodman, col. 7, lines 58-63 and col. 13, lines 45-53

19.   It would have been obvious to one of ordinary skill in the art at the time of invention that because Goodman detected whether an email was spam based upon the presence of a URL, and because therefore a URL would have been part of an email in Goodman, and because Milliken disclosed any portion of an email may be hashed, that a URL that was part of an email in Milliken would have been hashed.

20.   In regard to claim 6, Milliken disclosed the method of claim 4. Milliken, [0050],

hashing one or more portions of a received email. Milliken failed to disclose an

extracted URL was hashed.

21.   However, Goodman disclosed using the presence of a URL within an email to

determine whether an email was spam. Goodman, col. 7, lines 58-63 and col. 13, lines

45-53

22.   It would have been obvious to one of ordinary skill in the art at the time of

invention that because Goodman detected whether an email was spam based upon the

presence of a URL, and because therefore a URL would have been part of an email in

Goodman, and because Milliken disclosed any portion of an email may be hashed, that

a URL that was part of an email in Milliken would have been hashed.

23.   In regard to claim 7, Milliken disclosed the method of claim 4, wherein generating

the one or more signatures further comprises generating the one or more signatures

based on at least one of a protocol, a hostname, a domain name, a subsection of a

domain relative link, and an Internet Protocol (IP) address from the electronic

communication. Milliken, [0096], hashing specific headers from an email separately,

such as the use of Yahoo Groups

        In regard to claim 8, Milliken disclosed the method of claim 4, further comprising

classifying the electronic communication to be of the first predetermined category if one

of the selected signatures matches one of the plurality of predetermined signatures.

[0082], checking hashed portions of a message with known email lists which have been

hashed

24.   In regard to claim 9, Milliken disclosed the method of claim 4, wherein the

plurality of predetermined signatures is derived from a plurality of electronic documents

reported via a collaborative submission mechanism. Milliken, [0061], preloading of

hashes from "legitimate email list servers"

25.   Claims 15-19 are rejected under 35 U.S.C. 103(a) as being unpatentable over

Milliken in view of Goodman in view of Mitty et al in view of Knowles et al. (US

5,905,863).

26.   In regard to claim 15, Milliken disclosed a system comprising:

        a server, coupled to the plurality of databases, including: server 120, [0035]

                a memory device to store a plurality of instructions; and

                a processor, coupled to the memory device, to retrieve the plurality of

instructions from the memory device and to perform operations in response to

the plurality of instructions, the operations comprising:

                        generating one or more signatures of electronic communication

using a length of the electronic communication…; and Milliken, [0050],

where one or more portions of a received email are hashed to produce a

hash value. Any portion of the main text, or attachments may be hashed.

The hash acts as a signature in [0052].

                        determining whether the electronic communication is of a first

predetermined category using the one or more signatures generated.

Milliken, [0082], checking hashed portions of a message with known email

lists which have been hashed to determine if a message is spam or

suspicious.

Milliken failed to disclose hashing the URL extracted from a message.

However, Goodman disclosed using the presence of a URL within an email to

determine whether an email was spam. Goodman, col. 7, lines 58-63 and col. 13, lines

45-53

It would have been obvious to one of ordinary skill in the art at the time of

invention that because Goodman detected whether an email was spam based upon the

presence of a URL, and because therefore a URL would have been part of an email in

Goodman, and because Milliken disclosed any portion of an email may be hashed, that

a URL that was part of an email in Milliken would have been hashed.

Milliken failed to disclose generating a signature based upon a length of the

electronic communication. Milliken did disclose hashing can be performed on "one or

more header fields" of the email. [0050]. However, Mitty disclosed the generation of a

"unique waybill ID" [0067] which is a CRC of the encrypted message and a digest of the

encrypted message. The digest includes the "message length".

It would have been obvious to one of ordinary skill in the art at the time of

invention to include a message length in the digesting/signature creation/encryption of a

message in Milliken, as taught in Mitty, in order to improve the sorting techniques of

Milliken in regard to building a more robust spam prevention system.

Milliken and Goodman failed to disclose a plurality of databases to store a

plurality of signatures of a plurality of known electronic communications of a first

predetermined category. Milliken did disclose comparing known signatures of email

messages. Milliken failed to disclose the signatures compared were stored in a plurality

of databases.

However, Knowles did disclose use of multiple databases to compare message

content to determine if a message was a reply to another message. Knowles, column

5, lines 2-4 disclosed the multiple databases of different content, and column 5, lines

53-64 disclosed the querying of multiple databases of email content.

It would have been obvious to one of ordinary skill in the art at the time of

invention that Milliken's hash signatures would have been storable in a plurality of

databases for purposes of data backups and storage of different types of data.

27.   In regard to claim 16, Goodman disclosed the system of claim 15, wherein the

URLs comprises at least one of a hostname, a domain name, a subsection of a domain

relative link, and an Internet Protocol (IP) address. Goodman, col. 7, lines 58-63 and

col. 13, lines 45-53. The elements of at least one of a hostname, a domain name, a

subsection of a domain relative link, and an Internet Protocol (IP) address are inherently

part of the URL as disclosed in Goodman

28.   In regard to claim 17, Milliken disclosed the system of claim 15, wherein the

operations further comprise selecting the one or more of the plurality of signatures

based on a plurality of predetermined criteria. [0068], hash the main text of the body

and [0070], hash the attachments of the email. Also see [0050]. The use of hash

blocks in [0050] is selecting a signature generated based on a plurality of predetermined

criteria.

29.   In regard to claim 18, Milliken disclosed the system of claim 15, wherein the operations further comprise performing a predetermined operation on the electronic communication if the electronic communication is determined to be of the first predetermined category. Milliken, [0082], checking hashed portions of a message with known email lists which have been hashed to determine if a message is spam or suspicious.

30.   In regard to claim 19, Knowles disclosed the system of claim 15, further comprising a database, coupled to the server, to store a plurality of reports from which the plurality of predetermined signatures are generated. Knowles, col. 5, lines 55-58.

31.   Claim 20 is rejected under 35 U.S.C. 103(a) as being unpatentable over Milliken in view of Goodman in view of Knowles as applied to claim 15 above, and further in view of Applicant's Admitted Prior Art.

32.   In regard to claim 20, Milliken in view of Goodman in view of Knowles disclosed the system of claim 15. The combined references failed to disclose wherein the plurality of databases are in a remote location from the server. However, Applicant has admitted that prior art databases were commonly stored in remote locations from a server at the time of invention to allow for remote storage of data and for emergency management procedures in case of catastrophic events. It would have been obvious to one of ordinary skill in the art at the time of invention to remotely store databases in the Milliken/Goodman/Knowles combination.

Conclusion

33.   The prior art made of record and not relied upon is considered pertinent to

applicant's disclosure.

34.   Bisbee et al.   US 2012/0086971

35.   **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time

policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE

MONTHS from the mailing date of this action. In the event a first reply is filed within

TWO MONTHS of the mailing date of this final action and the advisory action is not

mailed until after the end of the THREE-MONTH shortened statutory period, then the

shortened statutory period will expire on the date the advisory action is mailed, and any

extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of

the advisory action. In no event, however, will the statutory period for reply expire later

than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the

examiner should be directed to Jeffrey R. Swearingen whose telephone number is

(571)272-3921. The examiner can normally be reached on M-F 8:30-5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's

supervisor, Lynn Feild can be reached on 571-272-2092. The fax phone number for the

organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Jeffrey R Swearingen
Primary Examiner
Art Unit 2445

/Jeffrey R Swearingen/
Primary Examiner, Art Unit 2445